Michigan Department of Community Health
HIV/AIDS Surveillance Program/Communicable Disease Division
Confidentiality and Data Security Policy

Section I: Legal Authority and Requirements

Reporting Law

In Michigan, HIV infection is required to be reported under Michigan Compiled Laws (MCL) 33.5114. AIDS is required to be reported under the Communicable Disease Rules that are promulgated by the Michigan Department of Community Health under MCL 333.5111.

Confidentiality

Both HIV infection and AIDS are designated as "serious communicable diseases or infections" under MCL 333.5101. MCL 333.5131(1) states that, "all reports, records and data pertaining to the treatment, reporting and research associated with [these] serious communicable diseases are confidential and shall be released only pursuant to this section. The exemptions are then listed and they are summarized in the booklet "Michigan HIV Laws, How They Affect Physicians and Other Health Care Workers".

Section II: Implementation of Policy

This policy will be reviewed annually and more often as necessary to insure that a review of evolving technologies occurs. The Security and Confidentiality Checklist Attachment-H (attached) from CDC's surveillance guidelines will be used to complete this review.

Overall Responsible Party (ORP)

The MDCH Deputy Director for Public Health Administration, Jean Chabut, MPH, is designated as the ORP and she will certify annually, as part of the CDC cooperative agreement application, that all security program requirements are met.

Breaches in Confidentiality

All staff authorized to access surveillance data are responsible for reporting suspected security breaches. Training of non-surveillance staff will include this directive. A breach of confidentiality must be immediately investigated to assess causes and implement remedies. A breach that results in the release of private information about one or more individuals (breach of

confidentiality) should be reported immediately to your supervisor who will report it to the Section Manager and the HIV/AIDS Epidemiology Manager. These managers must report this to the Reporting, Analysis, and Evaluation Team Leader, HIV Incidence and Case Surveillance Branch, DHAP-SE, NCHSTP, CDC. CDC may be able to assist the surveillance unit with the breach. In consultation with the appropriate legal counsel, surveillance staff should determine whether a breach warrants reporting to law enforcement agencies.

Personnel

This policy is given to and reviewed with all new employees. The policy is also kept in the office policy manuals in both the Lansing and Detroit offices. The policy is available to all employees at all times. As changes are made, updated policies are distributed to all employees and the office policy manuals are also updated.

Every individual with access to surveillance data must attend security training annually. IT staff and sub-contractors have limited access to data and have signed a confidentiality agreement with the State of Michigan and/or it's contractors. We are developing an annual standard training program for Department of Information Technology staff and/or other program contractors.

At Onset of Employment

Orientation of all new staff (including temporary, part time and/or contractual) includes comprehensive training on confidentiality requirements and related procedures. This training is prioritized to ensure that each employee fully understands the obligation and necessity of maintaining strict confidentiality in all aspects of their work, along with the proper ways to do so.

Confidentiality training includes:

1) Explanations of the federal guarantee of confidentiality upon which HIV/AIDS surveillance is based, and how it is essential to program success both nationally and at the state level, and how any infractions can result in harm to individuals as well as damage the confidence of the public and reporting contacts;
2) Review Michigan's state laws governing confidentiality of HIV/AIDS data and associated penalty for violation. Each employee is provided with a copy of these laws.
3) Review the confidentiality safeguards established within the HIV/AIDS Surveillance Section and specific office procedures that must be followed. Examples of ways to handle both routine and potentially compromising situations that may occur within the scope of each employee's duties are given. Each member of the surveillance staff must be responsible for protecting his or

her own workstation (hardcopy files and electronic computer files) associated with confidential HIV/AIDS surveillance information or data. This responsibility includes protecting keys, passwords, and codes that would allow access to confidential information or data. Staff must take care not to infect surveillance software with computer viruses.
4) Hardcopy of this policy will be given to each new employee.
5) Written oaths/attestation signed by each employee pledging to maintain confidentiality in accordance with all departmental practices and procedures; the pledge shall include information related to the fact that employees/contractor employees can be sued for breaches of confidentiality and may be liable for criminal penalties for such disclosures;
6) A written oath signed declaring that there are no potential conflicts of interest related to this employment.
7) Each member of the surveillance staff is responsible for questioning and challenging attempted use of data by unauthorized users and must also be responsible for reporting suspected security breaches;
8) Hardcopy documents containing confidential information will be shredded before disposing of them.

Annual Requirements for All Employees

1) Re-training in confidentiality policy and procedures; each employee shall sign an attendance sheet.
2) Undergo periodic performance review of adherence to confidentiality policy and procedures.
3) Renew oath to disclose any potential conflicts of interest.
4) The signed oath will be held in the employee's personnel file and a copy given to the employee at the time of signing.

At Resignation

Employees must sign a resignation list certifying they have returned all files, documents, office and file keys, identification badges, phone cards, voice mail passwords, laptops and other equipment to their supervisor. The supervisor will initial the list (to the left of each item) to indicate that they are in possession of each item. Failure to comply will result in a delay of the employee's final paycheck. All signed checklist document will be kept in each employee's permanent personnel file.

Section III: Record Retention of Identifying Information

1) Case report forms - maintain only 1 paper copy of each case report (2000xxx series copies are stored in the Lansing office while 4000xxx copies are kept in Detroit office [plus if an out state

resident then another copy is kept in Lansing]). Shred any extra copies and all records with confidential information before disposal.
2) Output records with patient names (paper and electronic files)- e.g., site line lists, registry matches, - as new ones are created, replace existing version. Review all lists annually at the time of the annual confidentiality training and destroy all lists > 1 yr. old.
3) Database archives to be limited to the following:
a) Network tape backups will be performed - i) daily, ii) weekly on Friday on a rotating basis, iii) monthly copies of this archived version will be maintained for a period of 6 mos.

Section IV: Operations and Management of Confidential Data

Access to Data

Access to confidential materials (electronic files and paper) shall be restricted to authorized surveillance staff. Authorized staff are those whose job duties require access to patient names. For the purposes of this policy unauthorized persons are defined as visitors or any member of the surveillance or other staffs (including housekeeping staff and building/maintenance staff) who do not have access to patient names as a part of their work duties.

All staff that are authorized to access surveillance data are responsible for questioning and challenging those who are not authorized to access surveillance data.

Access to local area network is granted via the department of information technology using a standard Network Request form that requires authorized management approval. Access to security and confidential information is then granted based on authorized surveillance job related duties.

Emergency Mode Operation

The availability of two different office locations (Lansing and Detroit) provides contingency office space in the case of emergency. The Communicable Disease Division has also identified the Office of Public Health Prepardedness location on Terminal Drive in Lansing, MI as a possible alternate location if needed. Staff will be notified and given directions via the Communicable Disease Division Continuity of Operations (COOP) Plan and the staff call tree regarding a change of office location during an emergency or power outage.

Physical Security

All surveillance staff authorized to access surveillance data are individually responsible for protecting their own workstation, laptop, or other devices associated with confidential surveillance information or data. This responsibility includes protecting keys, passwords, and codes that would allow access to confidential information or data. Staff must take care not to infect surveillance software with computer viruses and not to damage hardware through exposure to extreme heat or cold.

The building where Detroit staff are located is open to the public and consequently adherence to security measures that are carried out within the building is even more vital. The Lansing staff are in a locked suit on a secure floor requiring secure key fobs or identification to gain entrance. Neither the Detroit or Lansing offices are easily accessible by window.

For both Detroit and Lansing offices, eHARS is on the server located in Lansing and HARS is on the server located in Detroit and accessible via the dedicated T1 line utilizing a Wide Area Network (WAN). Other confidential databases are also stored on the Detroit server or the Lansing confidential folder. Computer access to the EHARS AND HARS and other confidential databases are approved only for surveillance staff with the appropriate assigned network rights (i.e., read and write access), based on their job duties. All computers are kept in locked rooms or suites with access limited to the surveillance staff. Access to the surveillance offices by cleaning staff and maintenance/building staff is routinely granted only during hours when authorized surveillance personnel are present or after all confidential materials are locked up and computer access is exited. More information on computer network security is discussed below.

Physical security risks for LAN installations center around three components: 1) servers; 2) workstations, printers and other peripherals; and 3) cabling. The physical area surrounding the LAN/WAN is protected against theft or misuse of the equipment or information.

The actual dedicated surveillance server(s) are physically located in a secured and restricted area within a locked server cabinet or secured server room. Only authorized staff have availability to keys to access this limited and restricted area.

Securing Data Outside of Offices

Regardless of the strength of our security practices in our offices, confidential information transported outside of the office can easily become the weak link in our system. Consequently, carrying named data out of the office requires specific supervisory/manager approval and must be kept to a minimum.

Release/Handling of Data

a) Surveillance information must be de-identified if taken out of the secured area for data analysis. A de-identified database must be held securely using password protected software. To de-identify a database, all names, social security number, address, and other potentially identifying information must be removed from the copy of the database. Furthermore, it is recommended that only variables necessary to the task at hand be included in the copy of the database.

Lists with names should only be taken into the field or home before a site visit the next day when absolutely necessary and every time must be approved by a manger or surveillance coordinator.

b) The information on lists that contain patient names should be kept to the minimum necessary. In any case there should not be any mention of HIV/AIDS. A numeric code will be used when the patient's diagnostic status is needed on the document.

c) Confidential computer files to be transported (sent electronically, via US mail or hand-delivered) must be encrypted and password protected.

d) All confidential materials must be shredded immediately following completion of use.

e) Other - refer to the following documents for further information:
>Policy on Release of Data to Outside Agencies >
>HIV/AIDS Surveillance Procedure Manual

Handling Paper with Patient Names/Lists

Confidential materials (including but not limited to case reports, supplemental surveillance and special project forms, and/or any paper with identifying information or lists of patient names) will be handled with the utmost care The amount and sensitivity of information contained in any one piece of mail must be kept to a minimum. Mailing labels and stamped envelopes will be supplied to local agency staff and providers to insure the use of correct mailing addresses and will not include the words "HIV or AIDS" or any similar reference. Whenever confidential information is mailed the envelope will be addressed to a specific 'named' person and clearly marked as confidential.

Below are some common situations and ways to avoid compromising confidentiality with written materials. These serve as examples only and are in no way meant to be an exhaustive list.

1) Materials with patient names (e.g., paper, phone messages, forms, etc):
a) are kept in locked file cabinets inside locked surveillance offices/suites and offices/suites that contain confidential material are locked whenever they are vacated during the day even if it is for a short time period;
b) are shredded using a crosscut shredder when they need to be discarded or disposed of in state approved locked containers for shredding by bonded outside state contractor
c) are not taken to private residences unless specific documented permission is received by a manager or surveillance coordinator. Each surveillance staff member will inform their supervisor annually or upon change about how they handle visits at each active site.
2) Prior approval must be obtained from a manger or the surveillance coordinator when business travel precludes the return of surveillance information with personal identifiers to the surveillance office by the close of business on the same day and are not left in cars; however, if it is absolutely necessary to leave it in an employee's car it should be kept locked in the trunk, if available and should also be locked in the trunk, if available, during transport; The vehicle should be parked in a locked garage, if available.
3) When case report forms are faxed they should **never** contain the patient's name or address or other identifying information. Identifying information should be communicated by telephone. Staff are alerted when faxes are being sent to stand at the fax machine to receive fax. The sender will be instructed to use a full cover sheet with the name and phone number of the recipient clearly marked. In Detroit, senders who are faxing confidential information should be given the number of the secure fax and not the general fax machine.
4) If an authorized staff person is working in eHARS the window using the flat "_" button in the upper right hand corner can be used to rapidly blank out the screen or the monitor can be turned off. (for HARS the F10 key can be used).
5) When confidential materials are handled in a room with open access (e.g., for copying) they are to be placed in a locked file when not in use and while being handled are kept out of view of unauthorized persons;
6) When these materials are handled in a private work area they are kept out of view of unauthorized persons. For example, line lists and case report forms should not be left on a desktop when authorized staff persons are out of the office.
7) Conversations about patients are carried on behind closed doors and are never carried out in any space (e.g., offices or hallways) when unauthorized persons are present;
8) Cases or names of potential cases are not discussed with anyone unless you know that the person already knows the patient's name and HIV/AIDS diagnosis.

a) Do not disclose the name of a patient living in one county with the local health department staff from another county unless the second county already knows the patient's name/diagnosis.

b) Do not reveal the names of suspect cases to health care providers unless there is reasonable evidence that that provider treated the patient.

9) Because of the potential number of entries on given paper copy line list, staff must exercise extreme caution before mailing.

Two methods that surveillance staff should employ to minimize the risk of breaching confidentiality are:

a. Generate list containing names without reference to HIV/AIDS.
b. Separate the names from other case information and mail the two separately.

Answering Telephone Inquiries and Knowledge of HIV Infection Status

Calls from sites requesting a check for a patient name in the registry are, in general, forwarded first to the person who is responsible for reporting from that site or, if not an enrolled site, from that county. If that staff person is not in, others can check the database with access to the EHARS registry*:* This may occur only under the following conditions:

Staff must always know to whom they are talking. Staff have been instructed to **never** give information about whether a person is or is not in the data base to someone over the phone unless they are sure they are who they claim to be; this can not be over stressed in importance.

When taking such calls it is preferable to give the person the information immediately over the phone. However, if it cannot be done while the person waits, staff may take the name(s) and date(s) of birth and 1) look it up later and call the person back or 2) pass on the list to the person responsible for that site.

When doing an eHARS Query, staff have been instructed that this is a one way flow of information - callers give us a name and we say what we do or do not know about that person. Do not say, No, I don't have John Doe but I have Steven Doe, since this inadvertently gives out information about other persons in the registry.

Knowledge of someone's medical status (HIV or other HIV-related medical information) obtained in either a work or social setting during or after one's work with the program is to be treated confidentially, i.e., not shared with persons outside of the program or with co-workers unless they have the need to know because of their surveillance responsibilities.

If an HIV/AIDS surveillance co-worker, employed with program, is reported as HIV positive, this case will be permanently entered into eHARS using a soundex code instead of name to protect confidentiality.

Identifiable information should not be left on voice mail. If surveillance staff need to use voice mail between Lansing and Detroit staff, a state number can be left but HIV/AIDS and the patient's name will not be mentioned. If staff need to discuss HIV and AIDS vital status, numeric codes one or two will be used respectively. Identifiable case follow-up information will not be left on external voice mail systems. Staff have been told to include instructions on their work voice mail message to callers telling them not to leave identifiable information as the

system may not be secure.

Section V: Electronic Security

The Network Administrator grants access to the Network Server that stores eHARS application and other confidential data on the server to authorized staff. The Database Manager and/or Laboratory Reporting Epidemiologist provides user rights to the eHARS reporting system. The network administrator periodically, no less than quarterly, will review user logs to identify potential unauthorized access.

Tape backups are stored in a secure fire protective cabinet with a locking mechanism.

All confidential data resides on the dedicated secure HIV/AIDS servers and confidential database files are not copied to individual workstations, hard drives, diskettes, memory jump drives, PDA's, other hand-held devices, or CD's from the servers.

No single connected modems are attached to non-laptop registry computers. Internet connections are only allowed through the State of Michigan Department of Information Technology protected Internet server and modem bank. Staff are instructed not to use the Internet at the same time that eHARS is open.

Patient identifiable surveillance information/data are not routinely stored on a laptop. If such data are copied to laptop, software that encrypts data as it is being copied will be installed on the laptop before use. Encryption is a method of protecting information from interpretation by unauthorized parties and must meet AES encryption standards. Encryption transforms information into an unrecognizable format. The key for decryption will not be on the laptop or kept in the case.

Surplus computers, diskettes, and data CD's - require special measures to remove hidden files/information on them; simple erase is not sufficient - A low density re-formatting of the hard drive wipes the entire hard drive or diskette clean of any contents.

Electronic transmission of data:

1) CDC data acknowledgments - refer to 'Data Transfer Protocol' in Database Management section of Procedure Manual
2) Any data that contain patient names or individual identifying information and are transferred electronically are password protected and/or encrypted and transferred to CDC using the Secure Data Network (SDN)..

3) Use of the state internal GroupWise E-mail system will be limited to internal communications between Lansing and Detroit HIV surveillance staff to update case information obtained in daily

work. Patient names and the use of the terms HIV/AIDS will not be used. Statenos can be used in the body of the message to refer to a specific patient. The subject line will say 'update' or some other non-descript phrase. The e-mail address will be doubled checked before the message is sent.

Computer Security

Network security is implemented at three levels:

User level: The Novell network requires each user to choose a unique password, and to choose a new password every 90 days. We require all users to maintain, at a minimum, a six-character password. Users are allowed to log in at any station, however they have been instructed to log off upon completion of work sessions at any workstation. Additionally, each workstation is configured with a password-protected screen saver, which will lock the computer after 5 - 10 minutes of non-use. This prevents entry by an individual who is not a part of the surveillance group.

Access to the network is available during regular business hours. Through the use of the Novell NetWare Time Restriction feature, access to the server on the weekend or evenings is available only upon request to the LAN Administrator.

Directory level: The network administrator limits access to entire directories and to individual files. The user can scan or open only those directories to which they have been given access. Only those staff members who are required to enter or change data in the database have write privileges to that file to protect it from erroneous data being entered.

Network level: The Network Administrator provides a User object (User ID and password) which is required for logging in to a network A User object represents a person who uses the network. The Administrator must assign user rights to resources, directory and files on the network file system.

Notebook/Laptop Computers

General policy does not permit the storage of personal identifying information on storage devices unless permitted by the Department Management and Security and Confidentiality Officer.

Laptops and other portable devices (e.g., PDAs, other hand-held devices, and tablet PCs) that receive or store surveillance information with personal identifiers must incorporate the use of encryption software meeting AES encryption standards. Surveillance information with identifiers must be encrypted. The decryption key must not be on the laptop or stored in the case.. Other portable devices without removable or external storage components must employ

the use of encryption software that meets Federal standards.

Following is a list of considerations when using laptops/notebook computers for surveillance purposes:

1) All backup and other disks are to be encrypted, and kept in a locked filing cabinet.
2) All files with identifying data are to be encrypted
3) No internal modems are allowed on non-laptop workstations
4) Data storage practices - in and out of office: locked briefcase or locked file cabinet if taken home.
5) Specify type of data to be stored on computer- should be only that which is essential to perform work
6) No laptop shall be operated for personal use

Data security involves a four tiered system: 1) Laptop Hard Drive Security Access 2) Remote Access Id and Password 3) data encryption, 4) user name and password.

Removable and Storage Devices; Memory sticks, Jump Drives and Floppy Diskettes

Do not store personal identifying information on removable storage devices unless specifically approved in writing by the Communicable Disease Division Director.

All removable or external storage devices containing surveillance information with personal identifiers or data from which a person could be identified must include only the minimum amount of information necessary to accomplish assigned tasks as determined by the surveillance manager/coordinator; be encrypted or stored under lock and key when not in use; and with the exception of devices used for backups, devices should be sanitized immediately following a given task. Before taking any device containing sensitive data out of the secured area, the data must be encrypted. Methods for sanitizing a storage device must ensure that the data cannot be retrievable using undelete or other data retrieval software. Hard disks that contained identifying information must be sanitized or destroyed before computers are labeled as excess or surplus, reassigned to non-surveillance staff, or before they are sent off site for repair.

Data files requested by and produced for local health departments are encrypted and password protected in all instances and mailed or hand delivered which is the preferred method.

Section VI: Data Release

Information that could identify an individual is not released. The Data Release Policy further discusses these related procedures.

Access to surveillance information or data for non-public health purposes, such as litigation, discovery, or court order, will be granted only to the extent required by law.

Section VII: Penalty for Violation

MCL Section 333.5131(8) states that "a person who violates this section is guilty of a misdemeanor, punishable by imprisonment for not more than 1 year or a fine of not more than $5,000.00 or both, and is liable in a civil action for actual damages or $1,000.00 whichever is greater, and costs and reasonable attorney fees. This subsection also applies to the employer of a person who violates this section, unless the employer had in effect at the time of the violation reasonable precautions designed to prevent the violation."

Violation of this written confidentiality and data security policy can result in immediate dismissal. In addition, supervisors may deny access to the named data bases at their discretion until necessary investigation occurs; for example, any employee who has data base access who exhibits questionable use or indiscretion will be denied access.

Section VIII: Conditions for Releasing Data to Collaborate with other Disease Registries
(Other MDCH Bureaus/Divisions, Michigan Cancer Society, TB and STD)

Access to HIV/AIDS surveillance information with identifiers by those who maintain other disease registries will be limited to those for whom the ORP has weighed the benefits and risks of allowing access and can certify that the level of security established by the other registry is equivalent to this policy.

Access to any surveillance information containing names for research purposes (beyond routine surveillance purposes) is contingent on a demonstrated need for the names, Institutional Review Board (IRB) approval, and the signing of a confidentiality statement regarding rules of access and final disposition of the information. Access to surveillance data or information without names may still require IRB approval depending on the numbers and types of variables in accordance with the data release policy.

Annually and periodically throughout the year, HARS and eHARS data are matched with data in other databases to improve data quality. eHARS (previously HARS) is matched annually with each of the following databases:

- Tuberculosis registry
- Birth registry

- Death registry
- Prison

And is periodically matched to the following databases:

- Cancer registry
- Medicaid database
- Syphilis
- Birth defects registry
- Social Security Death Master File

To protect the confidentiality of the data, all persons involved in linking these databases must undergo confidentiality training for both systems, if required, and sign any and all relevant oaths of confidentiality. Because of the nature of HIV data, where possible, all matches will be done by HIV surveillance staff, rather than other MDCH staff. In the event that the match is done by staff of the registry to which we are matching, their confidentiality standards must meet our requirements.

For the link with the Medicaid database, the match is done by MDCH Medicaid staff and the contractors that maintain the MDCH data warehouse. HIV surveillance data are included in a specific model that is only visible to approved HIV surveillance staff and the data warehouse IT staff. All IT staff members who may have access to HIV surveillance data must undergo HIV-specific confidentiality training and sign all required oaths of confidentiality. IT staff are held to the same requirements as HIV surveillance staff. Because this model is not visible to other warehouse users, there is no risk of them accessing the HIV surveillance data. Access to the data warehouse must be re-approved annually.

The live HIV database is never used to match to other databases. A copy of the live database is made first, and this copy is used for the match. In the event that an error in the match should occur, the original database will remain protected.

Other References:

Centers for Disease Control and Prevention and Council of State and Territorial Epidemiologists Technical Guidance for HIV/AIDS Surveillance Programs, Volume III: Security and Confidentiality Guidelines. Atlanta, Georgia: Centers of Disease Control and Prevention; 2006.

HIV/AIDS Surveillance Data Release Policy

MDCH Internet Policy Attached

State of Michigan Policy for Storage of Sensitive Information on Mobile Devices and Portable Media

State of Michigan
1315.00 Policy for Storage of Sensitive Information on Mobile Devices and Portable Media
Issued June 16, 2006

SUBJECT: Policy for Storage of Sensitive Information on Mobile Devices and Portable Media

APPLICATION: Executive Branch Departments and Sub-units, private partners and contractors.

PURPOSE: To establish a statewide policy for the protection of State of Michigan (SOM) sensitive information and data stored on mobile devices and portable media.

The public rightly assumes and should be assured that the data in the possession of Michigan state government is secure and protected from unauthorized disclosure or misuse.

CONTACT AGENCY: Department of Information Technology
Office of Enterprise Security

TELEPHONE: 517/241-4090

FAX: 517/241-2013

SUMMARY: Any user who has been authorized to access State of Michigan sensitive information has an obligation to safeguard and protect the confidentiality of such data. The objective of this procedure is to minimize the likelihood that sensitive or confidential SOM information is inadvertently disclosed.

PROCEDURE:

- Storage of sensitive information on mobile devices or portable media is permitted only if **all** of the following requirements have been satisfied:
  - Use is restricted to individuals whose job duties require it;
  - Granted for a finite duration as needed to fulfill the specific functions required to perform a specific job;
  - Approval has been obtained by both the employee's department head (or their designee) and the system/data owner. For non-SOM employees, "department" is defined as the SOM Agency contracting with the 3rd party;
  - Sensitive data has been encrypted. Encryption must comply with DIT Standard 1315.10 as published (http://www.michigan.gov/documents/1315_162702_7.10_Encryption_Policy.pdf). **Unencrypted storage of sensitive information on mobile devices and portable media is prohibited.** Please note that SOM Administrative Guide Procedure 1350.90 for data sanitation and media disposal will need to be followed.

- ANY instance of SOM sensitive information *(including that stored on a mobile device or portable media - encrypted or unencrypted)* being lost, stolen, or where there is reasonable belief that an unauthorized person may have acquired the data, **must be reported immediately** to your appropriate Agency management and the Department of

Information Technology's Customer Service Center (DIT CSC) at (517) 241-9700 or (800) 968-2644.

Terms and Definitions

Term	Definition
Data/system owner	Senior management of the Agency that is ultimately responsible for ensuring the protection and appropriate use of their business' data.
Encryption	The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key that enables you to decrypt it.
Term	**Definition**
Mobile devices	Any mobile device (State-owned or privately-owned) capable of storing data. Examples include, but are not limited to, laptop and tablet PCs, Blackberrys, cell phones, PDAs, IPods (MP3 players). For the purpose of this policy, all non-state-owned computing or data storage equipment (e.g., PC, server, NAS, SAN) are considered mobile devices.
Portable media	Any portable media (State-owned or privately-owned) capable of storing data. Examples include, but are not limited to, external hard drives, USB thumb drives, flash drives, memory sticks and cards, CDs, DVDs, floppy disks.
Sensitive information and data	Those data elements that are governed or restricted in some manner by a federal or state statute, rule, policy or requirement. **At a minimum, sensitive information that all Agencies must encrypt includes** (but is not limited to): ▪ **Name and social security number pair** ▪ **Name and credit card number pair** ▪ **Personal health records as identified by HIPPA** In addition to above, Agencies may assign data classifications to their data elements. Encryption would be required for any Agency-specific information labeled as sensitive.

- **Authority**

  E.R.O. No. 2001-1, compiled at § 18.41 of the Michigan Compiled Laws (Management and Budget Act 431 of 1984: Section 18, and Executive Reorganization Order 2001-1 now contained in the Act Section 18.41 Paragraph H).

- **Enforcement**

  Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment and/or criminal prosecution where the act constitutes a violation of law.

Any 3rd party found to have violated this policy may be subject to action, up to and including criminal prosecution where the act constitutes a violation of law. A breach of contract and fiduciary liability may also apply.

- **Exceptions**

  Exceptions to this policy may be granted solely by the Director of the Department of Information Technology (or the Director's designee).

- **Effective Date**

  Immediate upon release.

DEPARTMENT OF COMMUNITY HEALTH

Internet Policy

Access to the Internet has been provided to State employees for the benefit of the State of Michigan and its customers. It allows employees to connect to information resources around the world. Every staff member has a responsibility to maintain and enhance the State of Michigan's public image, and to use the Internet in a productive manner. To ensure that all employees are responsible, productive Internet users and are protecting the State's public image, the following policies have been established for using the Internet.

Acceptable Uses -

Employees accessing the Internet are representing the State. All communications should be for professional reasons. Employees are responsible for seeing that the Internet is used in an effective, ethical and lawful manner. Internet Relay Chat channels may be used to conduct official State business or to gain technical or analytical advice. Databases may be accessed for information as needed. E-mail may be used for business contacts.

Unacceptable Uses -

The Internet should not be used for personal gain or advancement of individual views. Solicitation of non-State business, or any use of the Internet for personal gain, is strictly prohibited. Use of the Internet must not disrupt the operation of the State network or the networks of other users. It must not interfere with your productivity.

Communications -

Each employee is responsible for the content of all text, audio or images placed or sent over the Internet. Fraudulent, harassing or obscene messages are prohibited. All messages communicated on the Internet should have your name attached. No messages will be transmitted under an assumed name. Users may not attempt to obscure the origin of any message. Information published on the Internet should not violate or infringe upon the rights of others. No abusive, profane or offensive language is transmitted through the system. Employees who wish to express personal opinions on the Internet are encouraged to obtain their own usernames through other Internet service providers.

Copyright Issues -

Copyrighted materials belonging to entities other than the State of Michigan, may not be transmitted by staff members on the Internet. One copy of copyrighted material may be downloaded for your own personal use in research. Users are not permitted to copy, transfer, rename, add or delete information or programs belonging to other users unless given expressed permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action from the State or legal action by the copyright owner.

MDCH/Bureau of Epidemiology
Approved June 10, 1997
Revised:
June 29, 2000; June 06, 2001; September 5, 2002, June 5, 2004; Oct. 17, 2005; Sept. 29, 2006
Confi06-092906final

Security -

All messages created, sent or retrieved over the Internet are the property of the State and should be considered public information. The State reserves the right to access and monitor all messages and files on the computer system as deemed necessary and appropriate. Internet messages are public communication and are not private. All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver.

Harassment -

Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual or group's race, religion, national origin, physical attributes, or sexual preference will be transmitted.

9/14/98

Michigan Department of Community Health (MDCH)
CD and Immunization Division - HIV/AIDS Surveillance Section

Employee Oath of Confidentiality

I, the undersigned, have read, understand and agree to abide by: the MDCH, BE, CDID, HIV/AIDS Surveillance Section Confidentiality and Data Security Policy and Michigan Complied Law (MCL333..5131(1) which states that all reports, records, and data pertaining to the treatment, reporting and research associated with serious communicable diseases including HIV/AIDS are confidential.

Furthermore, I understand that violation of these standards is subject to appropriate disciplinary action(s) on the part of MDCH, that could include being discharged from my position and/or being subject to other penalties. By initialing the following statements, I further agree that:

Initial Below

_____ Reports, records or information must be released in accordance with established policies.

_____ Any document to be disposed of that contains patients identifiers shall be shredded.

_____ All confidential files, including computer disk/cd, will be kept in a secured file cabinet when not in use.

_____ Any confidential files that I am working with will be locked up when I leave my workstation unattended.

_____ I will not receive visitors at any secure workstation when confidential information is out or visible.

_____ I will conduct telephone conversations and/or conference calls, requiring the discussion of identifiers, only in my secure work area or other confidential areas.

_____ When working on network files on my computer, I will log off when finished and leaving to prevent access to confidential files and databases.

_____ I will not disclose/give my computer password or office keys to unauthorized persons.

_____ Data generated and used while employed remains the property of MDCH and not the individual employee.

_____ I will not discuss any identifying information except in the performance of job-related duties, being especially mindful that these discussions do not occur in hallways, elevators, lavatories, lunch rooms or other public areas.

_____ Knowledge of someone's medical status (HIV or other HIV-related medical information) obtained in either a work or social setting during or after one's work with the program is to be treated confidentially, i.e., not shared with persons outside of the program or with co-workers unless they have the need to know because of their surveillance responsibilities.

_____ Infringement of these rules will be documented and placed in my personnel file.

_____ Upon leaving employment with the HIV/AIDS Section, I will return all items in compliance with elements on the resignation check list.

Employee Signature Date

I hereby certify that I have provided the above employee with a copy of the MDCH Policy regarding HIV/AIDS Surveillance Confidentiality and Data Security

Supervisor’s’s Signature Date